3GPP TSG SA WG3 Security — S3#10 **S3-000048**

19-21 January, 2000

Antwerpen, Belgium

3GPP TSG S3, N1, N2 ad hoc MAP security **TSGS3#*n*(00)*0010***
Darmstadt, Germany, 10-11. January 2000

Agenda Item:

Source: **Ericsson**

Title: **Enhancements on the extended Proposal for Securing MAP Based Transmission of Sensitive Data between Network Elements**

Document for: **Discussion**

Version: **2.2, 13th Jan 2000**

CONTENTS

1 Scope and Objectives

The security of the global SS7 network as a transport system for sensitive signalling messages is open to major compromise. Messages can be eavesdropped, altered, injected or deleted in an uncontrolled manner. The risk will be increased by the possible future use of open signalling protocols for signalling transmission (e.g. over TCP/IP under standardisation process in IETF sigtran WG). Even though in case of IP Technology IPSec can be used.

The present document proposes some enhancements to the CR 007 Ref.[1] where the general mechanisms for MAP security are outlined.

One premise on security analysis is that the weakest point in the security chain may compromise the complete security system. In signalling security the chain comprise a number of signalling protocols as ISUP, BSSAP, GTP, INAP, RANAP etc. Nevertheless the scope of this document only consider the CAP and MAP protocols as part of the protocols under the competence of SMG standardisation bodies. This limitation will simplify the discussion and similar principles could be applied to the remaining protocols.

2 Executive summary

This document presents a modified proposal for the implementation of MAP security. Key features of the modified proposal is based on:

- Definition of a new AMS (Authentication Mobile Server) entity that supports entity's authentication and key management.
- The Network entities generate a security relationship, called security binding in this document. This security binding provides:
    - Authentication of other end (Network entity) by use of upper level entities (AMS)
    - Session key agreements
    - Agreement on parameters to be encrypted (Mode to be used)
    - Agreement on messages to be authenticated (Mode to be used)
    - Algorithms to be used
    - Life time of session keys
    - Addresses that should use the specific security binding (i.e. Destination Network Element addresses)
    - …
- Backward and future proof proposal: Insertion of agreed parameters in a new parameter without modifying the format of the TCAP messages.

Differences:

The proposed solution in this document differs to the solution presented in the CR 007 mainly in the following points:

- This document proposes to generate a security binding where all the information needed is pre-established while the CR only proposes the session key agreement.
- The format of the messages is backward compatible without including any new layer in the SS7 stack.
- Solves the migration problem in a network (different vendors in the same network).

Benefits:

The solution in this proposal gives the following benefits:

- Allows a migration path for operators having different vendors in the network.
- Allows using of session key inside the network as well as with other networks.
- Allows inclusion of selected parameters for encryption or authentication depending on the needs of the operator.
- Allows Selection of functionalities (reduction of functionalities) depending on the support of cryptographic functions in other ends.
- Allows keeping the same format of the messages allowing backward compatibility.
- Allows using this solution even though different alternatives on transmission are available, such as IP (including IPSec.)

3 Justification

The risk analysis in reference [5] shows that the potential illegal activities using the signalling system affect to the user confidentiality, allow subscriber impersonating and compromise service availability of the network implying high economic impacts on the operator business.

The user confidentiality can be attacked basically acceding to certain information included in signalling messages. This information relates mainly to origin/destination of the calls and location of the subscriber. The risk has been increased in case of location by latest services allowing more accurate location information. In relation with confidentiality and possible fraud scenarios (not included in previous analysis) exist the possibility of alter the charging information transmitted using signalling protocols on CAMEL based services.

Regarding to subscriber impersonation the main threats are the manipulating of answers to authentication procedures and the eavesdropping of authentication information.

The service availability can be compromised at user or network level. The first one is based on manipulation of subscription information or messages granting the service. The second one can be originate by deletion of resource liberation related messages or overloading the network by message injection.

4 Problems

A part from the problems encountered and explained by the liaison statement N2-99F80 the following problems have been encountered in the CR Ref.[1]

- The evolution of networks with network entities from different vendors is not possible.

The change request does not solve the problem of identifying destination entities. This implies that the sending entity cannot select the protection mode for each message inside one network.

- Interworking with destinations that are in different networks and having different vendors has the same problem as in previous bullet.
- Protection mode 1 cannot be backward compatible with existing MAP protocol:

If it is backward compatible for the case that destination entity is not able to decrypt how could a session key for non supporting entities is generated?
If it is backward compatible, an insider can remove the security header and the Encryption/Integrity parameter and the destination entity will not notice it. This means that without a previous agreement, this protection mode is useless.

This contribution proposes enhancements to the existing CR so that the previous problems can be solved. The solutions consists mainly in introduction of:

- Security binding establishment phase were destinations, protection modes, session keys, etc are agreed
- A backward compatible MAP message format.

5 Requirements on the mechanism

The risks summarised below recommends to split the security signalling solution in three mechanisms fulfilling the corresponding requirements:

1. Data encryption: It is used to assure confidentiality of the transmitted information.

2. Authentication: It is used to assure that the messages received from certain entity has not been injected or replayed by intruders.

3. Integrity: It is used to assure that the information has not been manipulated.

The Protection Mode 1 in reference [1] implies the application of two mechanisms (i.e. authentication and integrity).

The Protection Mode 2 in reference [1] implies the application of three mechanisms (i.e. data encryption, authentication and integrity).

The main difference with the previous proposal, in reference [1], is that the information is considered important by itself, this implies that in some cases it could be desirable to use only data encryption (to avoid eavesdropping) or only data integrity (to avoid manipulation) independently of the other requirements.

In addition a support mechanism is needed to allow flexible handling of keys in which the encryption and authentication mechanism will be based.

Other requirements to be considered for the selected mechanisms are:

- Maintain the backward compatibility when communicating with entities not supporting the signalling security mechanism.

- Simplify the further development of the mechanism allowing the adaptation to further needs and technologies.

- Allows forward compatibility with possible further refinements of the mechanism (e.g. new encryption algorithms, future sensitive information transmitted, etc.)

- Minimise the possible impact on network performance.

- Minimise the number of entities in the network with high security requirements.

- Simple handling of roaming scenarios.

- High granularity on application of security mechanism at network, entity, procedure and subscriber level. Different security levels should be able to coexist.

- This mechanism should not preclude the application of other mechanisms like IPSec.

6 Overview on the mechanism

The field of key management is currently the aim of several investigation activities and standard proposals, so it is important to be able to adapt to these techniques with minimum impact on the UMTS system. Of course, a management system is proposed here and the encryption and authentication mechanism takes advantage of them in order to simplify the complete procedure.

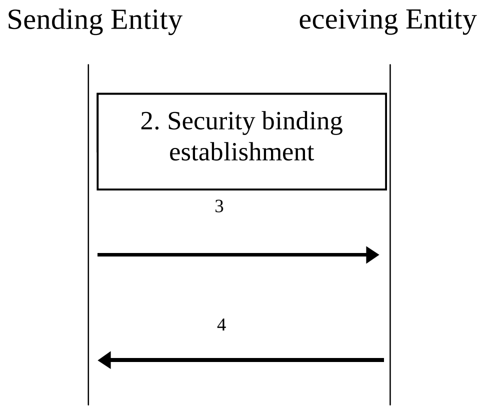
As justified in the previous section three mechanisms shall be defined (i.e. encryption, authentication, integrity and key handling). It is highly recommended that the aforementioned mechanism were as independent as possible is order to allow the independent application and simplifying the adaptation to emerging technologies.

6.1 General view

When two entities need to send and receive information, the mechanism consists on the following phases:

a) Establishment of a security binding between two network entities. This security binding provides an agreed session key, the parameters to be authenticated/encrypted, a lifetime of the session and some other information.
b) Selection of the functionality to be provided depending on the agreed security binding.
c) Sending and receiving MAP/CAP messages with the protected information according to the pre-established security agreement.

The following sequence shows the message flow corresponding to the transmission of protected parameters.



1. The sending entity checks that the security binding with the received entity has been established.
2. If the security binding is not established, or the life time has expired, the originating entity sends a *SecurityBindingRequest* message to the corresponding AUC
3. Message with encrypted information is sent.

The confidential parameters (identified by the security binding) are encrypted in the source node.

4. Message with encrypted information is answered.
   The answering node encrypts the confidential parameters (identified by the security binding).

The following messages do not request to establish the security binding.

6.2 Security binding establishment

6.2.1 Security management

In order to provide the signalling security mechanisms, a key distribution mechanism shall be provided.

It is very important to notice that the applicability of a standard mechanism, such as IKE, for key management should be taken into account.

The main problem for key distribution is the number of entities involved in the communication and the nature of them. The GSM/UMTS network allows roaming and that implies communication between several entities out of the operator security domain. On the other hand each operator may need to have complete control over the security in the entities.

In case a unique security binding are established with each network entity, the number of security bindings increases exponentially with the number of network elements. This will add complexity in processing so the trend should be to minimise the number of security bindings. A method to do this would be using the same session key for all (or a group) the security bindings. But if the same key is shared, the probability of breaking the session key increases. If that occurs, complete system security will be broken.

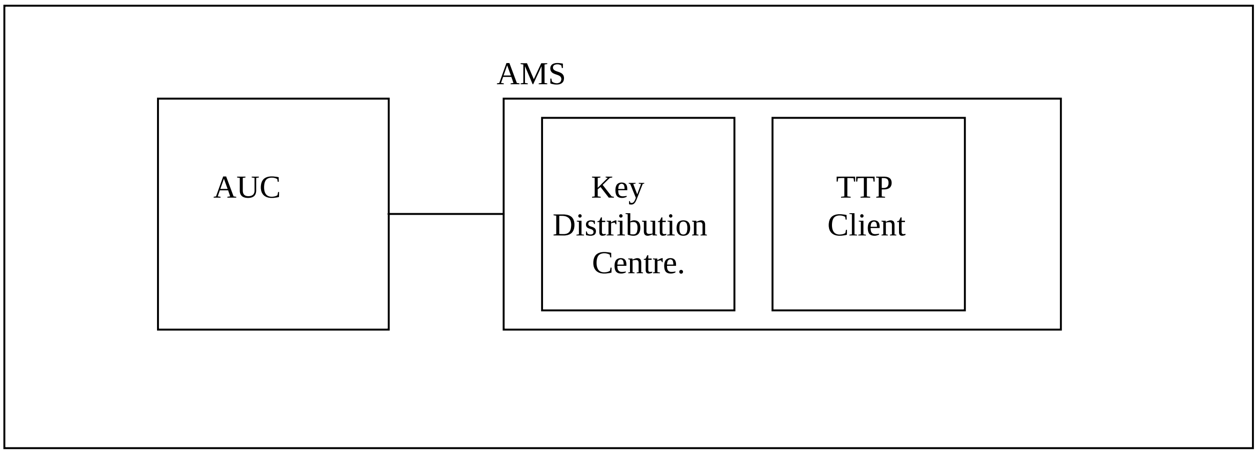
Depending on the amount of signalling to be sent, attacks based on massive information may occur. The amount of data to be protected with the same session key depends on the signalling between the two network elements, and on the number of security bindings using the same session key. Massive analysis only can be avoided by the use of very strong authentication mechanism, which usually are based on large keys and block sizes implying an undesirable impact in the system performance. Frequent changes of keys allow as well a good countermeasure against massive attack..

These reasons imply a compromise between the block sizes/key sizes and amount of data.

These conditions recommend that the number of entities, which shall be authenticated by Trusted Third Parties (outside the operator security domain), should be minimised. The proposal is to maintain only few entities in each GSM/UMTS networks that shall be authenticated by TTP systems.

The proposed solution is that the functionality of key handling in the operator domain shoild be based on the existing AUC entity. The main advantage of this solution is that the AUC should already fulfill strong security requirements that could be applicable also for this case. In addition AUC are handling MAP protocol that can be easily used for communicating entities (e.g. VLR, MSC, HLR, etc.) to handled key distribution.

A second view to this is to have a new specific entity of superior order to the AuC. This can be similar to the HSS view. This new upper entity could be an Authentication Mobile Server (AMS) that handles the new functionality:



The problem of attacks based on massive information can be avoid by frequent key changes as alternative to sophisticated and heavy algorithms. The use of session keys is highly recommended.

The basic key management architecture that shows the security bindings between network entities can be found in the following figure:

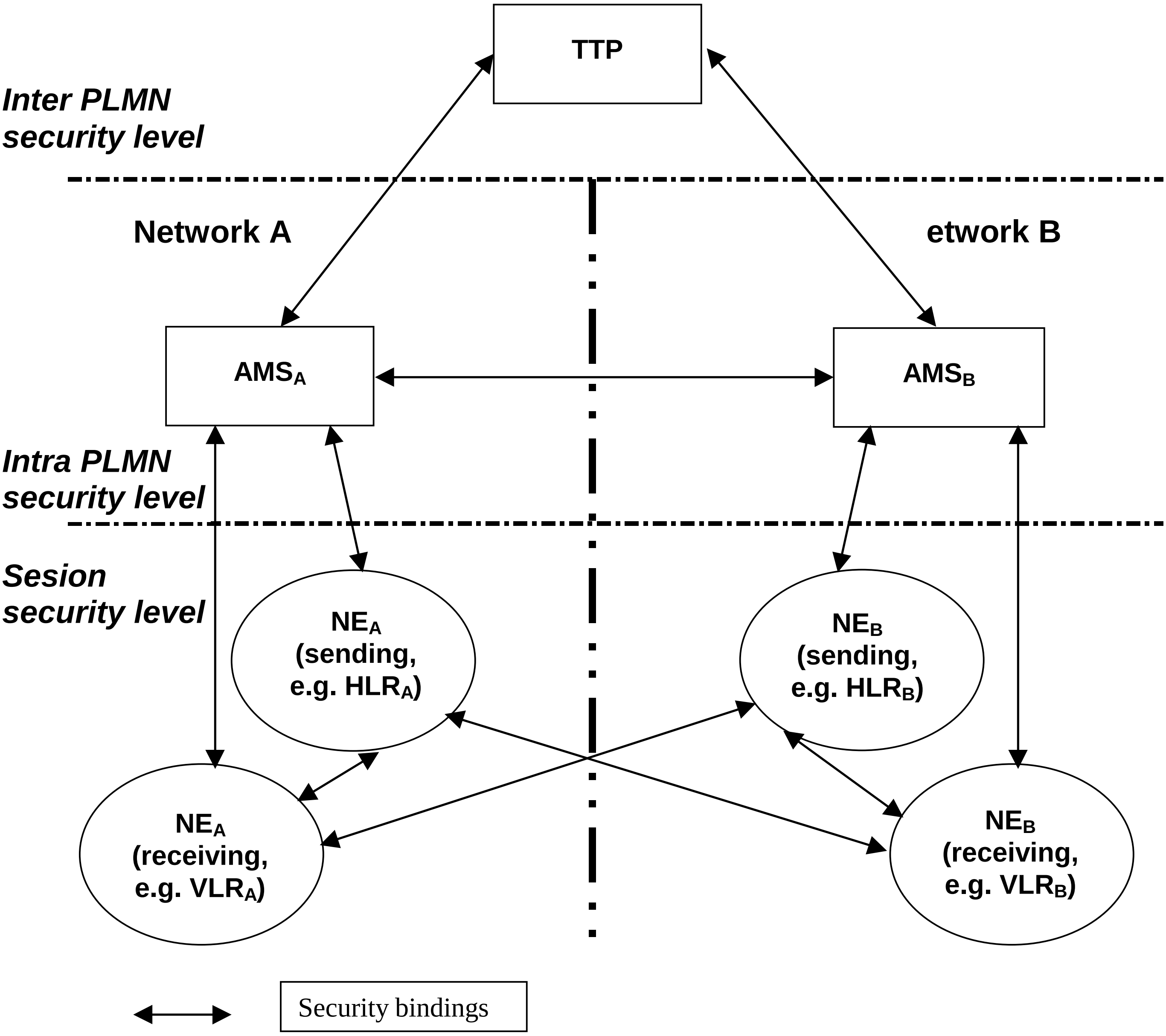

TTP
Inter PLMN security level
Network A
etwork B
AMS_A
AMS_B
Intra PLMN security level
Sesion security level
NE_A (sending, e.g. HLR_A)
NE_B (sending, e.g. HLR_B)
NE_A (receiving, e.g. VLR_A)
NE_B (receiving, e.g. VLR_B)
Security bindings

Figure 1: Overview of Proposed Mechanism

Three different security levels are defined:

1. Inter PLMN level:
   This level is used for establishing security bindings between entities belonging to different PLMNs. This should be based on either bilateral agreements between PLMN operators or by trusting in an external corporation or entity acting as TTP. These security bindings have strong security requirements and the specific mechanism used should be sufficiently flexible to allow state of the art techniques. The TTP could be integrated with other systems outside GSM/UMTS (e.g. between ISP, etc) and from this point of view it is not recommended that the corresponding interfaces are standardised. Nevertheless a default

mechanism, similar to the proposed for inter PLMN level, should be supported to provide this security bindings in a multivendor environment from day one without dependencies form other standardisation bodies.

2. Intra PLMN level:
   This level is used for establishing security bindings between entities belonging to the same PLMN. This should be based on one or more AUC entities (with security bindings established) which acts as TTP for the entities in the PLMN. These security bindings should be able to be established under operator premises. So the selected mechanism should allow the establishment of different standardised and/or customised security schemas. Nevertheless some standard mechanisms should be supported to provide this security bindings in a multivendor environment. The proposal is to base the selected mechanism in MAP protocol.

3. Session level:
   This level is used for establishing security bindings between communicating entities. The proposal is to base the selected mechanism in MAP protocol. The session established will be handled through the entities‘ in inter PLMN layer (AUC). Each entity trust in their corresponding AUC.
   Two cases depending of the type of communication (inter PLMN or intra PLMN) are envisaged.
   - Inter PLMN: The selected mechanism should allow the establishment of different standard security schemas
   - Intra PLMN: The selected mechanism should allow the establishment of different either standard and customised security schemas. Nevertheless some standard mechanisms should be supported to provide this security bindings in a multivendor environment.

So the selected mechanism should allow the establishment of different either standard and customised security schemas. The proposal is to base the selected mechanism in MAP protocol.

6.2.2 Security binding data

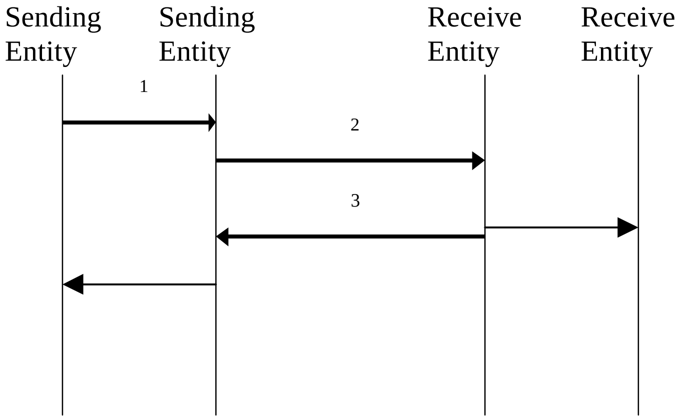
The security bindings between entities indicate the allowed communication between entities and the characteristics of the *Encryption, Authentication, Integrity* mechanism used and specific characteristics of the corresponding binding.

They will include:

- *Binding Identity*: Unique identification of the security binding in the corresponding domain.
- *Encryption*: Parameters to be encrypted/protected, the algorithms applicable (e.g. BEANO) and the session key used.
- *Authentication:* Messages requiring authentication, the authentication system applicable and the key used.
- *Integrity:* Messages requiring Integrity and the integrity system applicable.
- *Live time*: The time during which the security binding is considered applicable.
- *Destinations*: A list of addressees or group of addressees (e.g. MSISDN series) included in this security binding.

6.2.3 Message sequence

The following sequence shows the message flow corresponding to the transmission of *Integrity* Information.



1. The sending entity checks that the security binding with the received entity has not been established or has expired.
2. The originating entity sends a *SecurityBindingRequest* message to the corresponding AUC.
   The AUC maintains information about the desired security bindings for the sending entity (it will indicate for each attribute if they are requested or negotiable)
3. The originating AUC sends a *SecurityBindingNegotiation* message to the corresponding AUC of the receiving entity.
4. The AUC of the receiving entity answer with the accepted security binding attributes.
5. The negotiated security binding are notified to the sending and receiving entities by a *SecurityBindingNotification* message and the communication can be initiated.

6.2.4 Messages format

The key handling messages shall be send encrypted, authenticated and with integrity information included following the same principles than above.

First messages between the network entity and the AuC might be based on a secret key. Other security protocols can be used instead.

6.3 Security level decision

Once the security binding has been established, the network element may decide to restrict certain information because the other end does not support the security level required. For example, if location information is requested and the receiving entity does not support encryption for this information, the sending entity may decide not to send it.

6.4 Sending of encrypted data

6.4.1 Data encryption

Some confidential information are Location information, Charging information and authentication vectors (other are calling and called number, etc.) this information are identified in MAP and CAP protocols in the following messages:

Location information

Parameter	***Message***	***Protocols***
RESULT parameter:locationInformation	ProvideSubscriberInfo (HLR->MSC/VLR)	MAP V1,V2,REL96, REL97
RESULT parameter:locationInformation	SendRoutingInfo (HLR ->GMSC)	MAP REL96, REL97
RESULT parameter:locationInformation	AnyTimeInterrogation (gsmSCF -> HLR)	MAP REL96
ARGUMENT parameter: locationNumber	InitialDP (gsmSSF -> gsmSCF)	CAP

Geographical co-ordinates are under standardisation process in Location Services WI.

Charging information

Parameter	***Message***	***Protocols***
RESULT parameter PartyToCharge	FurnishChargingInfo (SCF->SSF)	CAP REL97
RESULT parameter FreeFormatData	FurnishChargingInfo (SCF->SSF)	CAP REL97

Authentication vectors.

Parameter	***Message***	***Protocols***
RESULT parameter: AuthenticationSet	SendAuthenticationInfo (MSC/VLR -> HLR, VLRa -> VLRb)	MAP V1,V2,REL96, REL97

The first consequence of the examples above are that the parameters are not present in all the messages and that usually they are only an small part of the complete message requesting such confidentiality.

In addition, it shall be considered that the information used for addressing purposes (e.g. at SCCP) can be accessed at lower levels than MAP or CAP protocols (e.g. IMSI, MSISDN, VLR number, etc). As consequence, the security chain for this information is vulnerable and does not make sense to protect at Application Part level.

It should be noticed that this information could be present in lower layers, for example used for routing on SCCP, and should be protected as well.

The proposed mechanism for data encryption is based on encryption of the confidential information at parameter level removing these parameters from the *ClearText* part and including in a new *Encrypted* part of the MAP operation e.g.

Param_1, Param_2, Param_3, Param_4

If *Param_2 and Param-4* are confidential

ClearText(Param_1, Param_3), Encrypted(Param_2,Param_4)

It is very important to notice that inside the encrypted information parameter, it is not included only the protected parameter, but there can be some TVP or other in clear text that supports correct handling of encryption. This part is already studied in the CR Ref[1] that can be reused.

6.4.2 Entity authentication

Some operations may cause undesired behaviour in the network when injected by impersonating trusted entities.

In principle all operations may be used with illegal purposes. Some examples could be:

Message	***Effect***	***Protocols***
UpdateLocation (VLR -> HLR)	Allow originating services to not registered subscribers	MAP
ProvideSubscriberInfo (HLR->MSC/VLR)	Allow un-allowed terminating calls	MAP
InsertSubscriberData (HLR ->VLR)	Allow services not provided to the subscriber. Allow arming CAMEL TDPs.	MAP
InterrogateSS (HLR ->VLR)	Request subscriber information.	MAP
AnyTimeInterrogation (gsmSCF -> HLR)	Request subscriber information.	MAP
InitialDP (gsmSSF -> gsmSCF)	Its interception allows overcome possible controls.	CAP

The first consequence of the examples above are that the different messages may have different influence in the network behaviour and as consequence not all entities has the same authentication requirements.

Other consequence is that depending on the operation the invoking or answering entity may request authentication (e.g. in LU the receiving, in ISD the sending, etc.).

In addition, it shall be considered that the information used for addressing purposes (e.g. at SCCP) can be accessed at lower levels than MAP or CAP protocols (e.g. IMSI, MSISDN, VLR number, etc.) and changed. The consequence is that the security chain based on policy functions on lower levels can be overcome and the system is vulnerable.

Due to the implementation of CAMEL based applications, modification of the supplementary services provided to certain subscribers may occur in case that the network entities are not authenticated.

The proposed mechanism for entity authentication is based on an authentication per entity applied only to select operations a new *Authenticator* parameter will be included in the new *Encrypted* part of the MAP operations.

Param_1, Param_2

If the sending entity will be authenticated

ClearText(Param_1, Param_2), Encrypted(Authenticator)

6.4.3 Data Integrity

The integrity of the information will be assured. This should be including some *Integrity* information in the *Encrypted* part of the MAP operation calculated based in the message content and other potential information (e.g. TVP, time stamp, sequence number, etc.). The operation in the example will appear as:

Param_1, Param_2

If the message integrity will be assured

ClearText(Param_1, Param_2), Encrypted(Integrity)

Supplementary Service information

Message	***Effect***	***Protocols***
InsertSubscriberData (HLR ->VLR)	Allow services not provided to the subscriber. Allow arming CAMEL TDPs.	MAP

Charging information

Parameter	***Message***	***Protocols***
RESULT parameter PartyToCharge	FurnishChargingInfo (SCF->SSF)	CAP REL97

RESULT parameter FreeFormatData	FurnishChargingInfo (SCF->SSF)	CAP REL97

7 Phase implementation

Due to the complexity of the system, it should be implemented in phases reducing the functionality to the minimum required on each case. For example, a first phase should implement default encryption algorithms with only one key with selected networks. This would allow reducing the impacts on the network as the security binding is pre-established and not changeable.
A further development would allow modifying the network requirements.

8 Conclusion

This contribution solves the problems encountered in the CR Ref [1], but there is a big list of pending activities that must be solved for the conclusion of the work.

The activities to be further studied in the MAP security area are:

- A detailed list of parameters/messages to be encrypted/Authenticated.
- A detailed study of the protocols to be used in the layers I and II.
- Detailed procedures when one system recovers.
- A deep study of the different algorithms to be used for signalling and the impacts on the behaviour in the network elements.
- Increase of length in the messages in octets and use of different SCCP releases.
- Detailed method to introduce the encrypted parameters in MAP protocol.
- Modifications to the TS 33.102 because of this new approach.
- Modification to the TS 29.002 with the new parameters.

9 References

[1] CR 007 to the TS 33.102 v 3.0.0 Date 99-06-18.

[2] ETSI GSM 09.02 Version 4.18.0: Mobile Application Part (MAP) Specification.

[3] ISO/IEC 11770-3: *Key Management – Mechanisms using Asymmetric Techniques*.

[4] ETSI SAGE: Specification of the BEANO encryption algorithm, Dec. 1995 (confidential).

[5] SS7 Signalling Protocols Threat Analysis, Input document AP 99-28 to SMG10 Meeting #28, March 99, Stockholm.

10 Abbreviations

The following abbreviations are used in this document:

BEANO	Block Encryption Algorithm for Network Operators
MAP	Mobile Application Part
SCCP	Signalling Connection Control Part